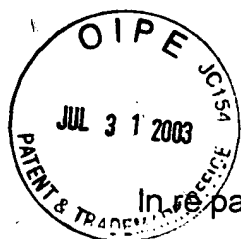


AF 13627



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re patent application of:

) Date: July 29, 2003

Frank S. Saavedra-Lim

) Attorney Docket No.: E-833

Serial No.: 09/475,950

) Customer No.: 00919

Filed: December 31, 1999

) Group Art Unit: 3627

Confirmation No.: 7103

) Examiner: Gerald J. O'Connor

Title: **METHOD AND SYSTEM OF UPGRADING THIRD PARTY  
FUNCTIONALITY IN AN ELECTRONIC FRAUD MANAGEMENT  
SYSTEM**

**RECEIVED**  
AUG 04 2003  
**GROUP 3600**

**TRANSMITTAL OF CORRECTED APPEAL BRIEF (PATENT APPLICATION 37 CFR  
1.192)**

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

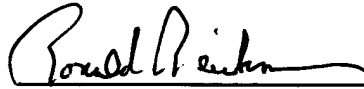
Sir:

Transmitted herewith in **triplicate** is the **CORRECTED APPEAL BRIEF** in the above-identified patent application with respect to the Notice of Appeal filed on March 4, 2003, and the Office Action mailed July 11, 2003.

The Commissioner is hereby authorized to charge any additional fees which may be required to Deposit Account No. **16-1885**.

A duplicate copy of this transmittal is enclosed for use in charging the Deposit Account.

Respectfully submitted,



Ronald Reichman  
Reg. No. 26,796  
Attorney of Record  
Telephone (203) 924-3854

PITNEY BOWES INC.  
Intellectual Property and  
Technology Law Department  
35 Waterview Drive  
P.O. Box 3000  
Shelton, CT 06484-8000

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

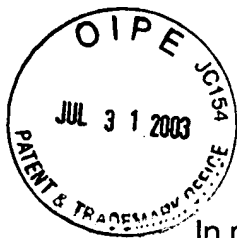
Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

on July 29, 2003  
Date of Deposit

Esther A. Lapin  
Name of Rep.

  
Signature

July 29, 2003  
Date



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**RECEIVED**  
AUG 04 2003  
**GROUP 3600**

In re patent application of:

) Attorney Docket No.: E-833

Frank S. Saavedra-Lim

) Group Art Unit: 3627

Serial No.: 09/475,950

) Examiner: Gerald J. O'Connor

Filed: December 31, 1999

) Date: July 29, 2003

Confirmation No. 7103

) Customer No. 00919

Title: **METHOD AND SYSTEM OF UPGRADING THIRD PARTY  
FUNCTIONALITY IN AN ELECTRONIC FRAUD MANAGEMENT  
SYSTEM**

**APPELLANT'S CORRECTED BRIEF**

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P. O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This Corrected Brief is in furtherance of the Notice of Appeal filed in this case on March 4, 2003, and the office action mailed July 11, 2003.

This Corrected Brief is transmitted in triplicate.

## **TABLE OF CONTENTS**

This Corrected Brief contains these items under the following headings and in the order set forth below.

- I. REAL PARTY IN INTEREST
- II. RELATED APPEALS AND INTERFERENCES
- III. STATUS OF CLAIMS
- IV. STATUS OF AMENDMENTS
- V. SUMMARY OF INVENTION
- VI. ISSUES PRESENTED FOR REVIEW
- VII. GROUPINGS OF CLAIMS
- VIII. ARGUMENTS
- IX. PRAYER FOR RELIEF
- X. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

## **I. REAL PARTY IN INTEREST**

Pitney Bowes Inc. is the real party in interest.

## **II. RELATED APPEALS AND INTERFERENCES**

There are no related Appeals and interferences.

## **III. STATUS OF CLAIMS**

- a) Claims 1 – 6 and 9 -10 are in the application.
- b) Claims 7 and 7 have been canceled.
- c) Claims 1 – 6 and 9 -10 are rejected.
- d) Claims 1 – 6 and 9 -10 are on appeal.

## **IV. STATUS OF AMENDMENTS**

An Amendment subsequent to the Final Rejection of December 3, 2002, was filed on March 4, 2003. This Amendment was entered.

## **V. SUMMARY OF THE INVENTION**

### **A. Background**

**Prior art methods did not assess a set of risks relative to granting credit on a financial product by applying a fraudi to each assessment wherein the fraudi is selected from a list of fraudi that is representative of a defined area of risk.**

Within the financial industry in general there is a marked propensity for fraud, which thus associates a certain degree of risk with each transaction or

financial product introduction. This is particularly true in the credit card portion of the industry. Case history supports this conclusion. Fraud can, and does, originate both internally to the organization issuing the financial product, and externally, with customers, vendors, merchants, or criminals that intercept the communication of credit card information, electronically, or physically. Thus, fraud in this industry is expected.

Fraud is inherent in how credit cards are issued and handled. There is, for example, no significant threat to the issuer of a card from someone finding a lost credit card and using it to purchase gas in an automated gas station; and, telephone and mail orders may be made by criminals illegally possessing credit account information. In the same category, a fraudulent merchant may be operating fraudulently by selling merchandise on unequal consideration. On a larger scale, however, fraud rings are particularly active and include many players in their networks that defraud issuers of billions of dollars. Rogue employees and questionable merchants account for a significant part of skimming activity, which involves the illegal acquisition of account information in order to produce counterfeit cards or make fraudulent transactions. The sophistication of skimming is quite advanced in that criminals may wait up to eighteen to twenty (18-20) months after skimming a card before they use it. This category of fraud which originates at the point of sale is expected to be a twenty-five billion dollar (\$25,000,000,000) problem in 1999.

Recent security conference statistics show that distinct trends emerge from studies of fraud. The top fraud types are lost, stolen, or counterfeit credit cards or accounts. Fraud losses resulting from lost and stolen credit cards (plastic) represent nearly sixty percent (60%) of all losses, with the fourth (4th) quarter of any year being the top fraud period. The hours of 12:00 Noon to 10:00 PM are the peak fraud activity times; California, Florida and New York are the top fraud states; and, Los Angeles, New York City, and Las Vegas are the top fraud

cities. Telemarketing, phone use, and gas purchases are the top fraud industry groups.

While it is evident that fraud exists, and that it is extremely difficult to eliminate, even in the current technological environment, actions can be taken to control the impact of fraud.

The credit card industry is not totally defenseless when it comes to fraud. It is evident that acquirers (merchants), issuers (banks), the major credit card associations (i.e., VISA® and MasterCard®), and third party vendors are making their best efforts to stay on top of the issue. The theme of fraud management is currently one promoting early detection and warning and loss mitigation as close as possible to the point of sale. There are a number of industry tools that are being employed to manage fraud and risk accordingly.

Applications for credit cards undergo scrutiny from such industry watchdogs and utilities as the VISA ICS (Issuer's Clearinghouse Service), from general information validation procedures, and from credit bureau fraud screen products such as SAFESCAN from Equifax, HAWK from TransUnion, or FACS from Experian. Transaction processing too, undergoes scrutiny from such industry methods as: the Fair Isaac Consumer Score (FICO); the Falcon - Neural Network Model (HNC); NESTOR - Neural Network Model; Queue Based Fraud Detection (TSYS DFS); the VISA Consumer Risk Score (CRIS); and, the VISA Magnetic Code Verification (CVV/CVC).

While the industry has taken steps to safeguard against fraud, it is recognized that the existing fraud detection technology (such as making calls to cardholders when a fraud is suspected) can impact desired customer service and convenience. Therefore, a balance is required in the state of fraud management that will allow the industry to protect itself while remaining commercially viable.

One aspect of progressive fraud management is the development of a concept, structure and effective method for allowing fraud to be identified, measured, and proactively managed at the task level. Another requirement for effective fraud management is the development of an ability to benchmark against the industry.

**B. Appellant claims a method that assesses a set of risks relative to granting credit on a financial product by applying a fraudi to each assessment wherein the fraudi is selected from a list of fraudi that is representative of a defined area of risk.**

According to the invention, the object is achieved and the disadvantages of the prior art are overcome by a method for managing and assessing a set of risks relative to a financial product, wherein the method is accessed through a data processing system. The data processing system comprises a series of nodes operatively connected with each other. The method begins by performing an application processing procedure, comprising a check of the creditworthiness of one or more selected customers; and issuing a financial product to the selected customer if that customer is determined to be creditworthy; and, declining the application if the customer is determined to be not creditworthy.

After the card has been issued to a customer, the use of the card is assessed whenever the card is presented for payment of goods or services or to obtain a cash advance. The assessment is made as the result of a credit authorization request from a merchant or a system user and utilizes a predictive modeling routine to perform the assessment. The credit authorization is accepted or rejected based upon an outcome of the assessment. The assessment results are then downloaded to the data processing system for transfer to a database accessible by one or more remote nodes of the system.



The assessment itself further comprises the steps of applying a transaction procedure to determine whether or not the credit authorization request is to be accepted or declined, and then applying a fraudi set to the assessment methodology. The fraudi set serves to identify a set of risks associated with each step of the assessment. The credit authorization assessment methodology further comprises the steps of: performing a set of pre-processing checks; performing a set of transaction approval checks; performing a set of post processing checks; and, making a set of post approval account adjustments required as a result of a credit authorization approval. On an individual transaction basis, each transaction can be accepted or declined based upon an outcome of the assessment.

Any of the transactions, assessments, or determinative calculations can be retained as a means of continually refreshing the pool of data available for credit determinations.

This invention claims a method that assesses a set of risks relative to granting credit on a financial product information, which is shown in Fig. 10 and was added to page 28, of the specification. After the program starts, the program goes to block 900. In block 900, the program performs an application procedure, comprising a check of the creditworthiness of one or more selected customers; and issuing a financial product to said customer if said customer is determined to be creditworthy, resulting in an accepted customer, and declining said application if said customer is determined to be not creditworthy. Then the program goes to block 901 to assess a credit authorization request from a merchant or a system user, where said request is initiated by a user of said financial product. Now the program goes to block 902 to select a fraudi from a list comprising one or more fraudi and wherein said each one of said fraudi is representative of a defined area of risk. Then the program goes to block 903 to apply the selected fraudi to each one of said assessment steps. Then the program goes to block 904 to

utilize a predictive modeling routine to perform said assessment. Now the program goes to block 905 to accept or decline said credit authorization request as based upon an outcome of said assessment. Then the program goes to block 906 to download said assessment result to said data processing system for transfer to a database accessible by one or more remote nodes of said system.

## **VI. ISSUES PRESENTED FOR REVIEW**

- A. Whether or not claims 1 - 3 are patentable under 35 USC §102(e) over Walker, et al. (U.S. patent No. 6,664,987).
- B. Whether or not claim 4 is patentable under 35 USC §102(e) over Walker, et al. (U.S. patent No. 6,664,987).
- C. Whether or not claim 5 is patentable under 35 USC §102(e) over Walker, et al. (U.S. patent No. 6,664,987).
- D. Whether or not claim 6 is patentable under 35 USC §102(e) over Walker, et al. (U.S. patent No. 6,664,987).
- E. Whether or not claim 9 is patentable under 35 USC §102(e) over Walker, et al. (U.S. patent No. 6,664,987).
- F. Whether or not claim 10 is patentable under 35 USC §102(e) over Walker, et al. (U.S. patent No. 6,664,987).

## **VII. GROUPING OF CLAIMS**

- A. Claims 1 - 3 stand or fall together with regard to the rejection under 35 U.S.C. §102(e).

- B. Claim 4 stands or falls by itself with regard to the rejection under 35 U.S.C. §102(e).
- C. Claim 5 stands or falls by itself with regard to the rejection under 35 U.S.C. §102(e).
- D. Claim 6 stands or falls by itself with regard to the rejection under 35 U.S.C. §102(e).
- E. Claim 9 stands or falls by itself with regard to the rejection under 35 U.S.C. §102(e).
- F. Claim 10 stands or falls by itself with regard to the rejection under 35 U.S.C. §102(e).

## **VIII. ARGUMENTS**

- A. Claims 1 - 3 have been rejected by the Examiner under 35 USC §102(a) as being unpatentable over Walker, et al. (U.S. patent No. 6,664,987).**

Walker discloses the following in lines 11-41 of column 3:

"In accordance with the present invention, a central controller receives from a POS terminal a purchase price and a financial account identifier. The financial account identifier specifies a financial account, such as a credit card account. The central controller, in turn, generates one or more installment plan identifiers indicating installment plans for payment of the purchase price. The installment plan identifiers are based on the purchase price and/or the financial account identifier. For example, certain accounts or certain high purchase prices may merit preferred installment plans. The installment plan identifiers are transmitted to the POS terminal.

A purchaser at the POS terminal selects whether he would like to pay for his purchase in installments and, if so, using which installment plan. The POS terminal generates a selection signal indicative of whether to accept any of the installment plans. In other words, the selection signal indicates a selected one of the installments plans (if the purchaser desires to pay in installments) or that no installment plan was selected. The POS terminal then transmits the selection signal to the central controller.

The central controller receives the selection signal. If the selection signal indicates acceptance of any installment plan, use of the accepted installment plan for the financial account is authorized. Thereafter, bills are generated which reflect installment charges to be paid. Thus, the purchaser may afford more purchases than otherwise possible, and may utilize such installment payments for purchases bought at many sellers."

In essence, Walker is disclosing a method for allowing purchasers to select an installment plan for the purchasing of goods so that the purchasers may spread out their payments over time. Walker does not disclose or anticipate the invention claimed by Appellant in claim 1, and those claims dependent thereon. Appellant claims a method of managing and assessing a set of risks relative to a financial product. Appellant is assessing a credit authorization request from a system user, wherein said request is initiated by a use of said financial product; utilizing a predictive modeling routine to perform said assessment; accepting or declining said credit authorization request as based upon an outcome of said assessment; downloading an assessment result to said data processing system for transfer to a database accessible by one or more remote nodes of said system; and applying a fraudi to each assessment and wherein said fraudi is selected from a list of fraudi and wherein each of said fraudi on the list is representative of a defined areas of risk. Walker is not concerned with the

assessing of risks for a financial product. Walker is concerned with providing a method for allowing purchasers to select an installment plan for purchasers at a time of sale.

Each of the said frauds on the list is representative of a defined area of risk that is listed in Fig. 3, i.e.:

- Account Closure - Fraudulent Reinstatement of Account
- Account Disputes and Chargebacks
- Account Information Changes in Writing - Address
- Account Information Changes Via Telephone - Adding Cardholder
- Account Information Changes Via Telephone - Address
- Account Information Changes Via Telephone - Business Name
- Account Information Changes Via Telephone - Abuse of Closed Account
- Account Information Changes Via Telephone - Cash Access Employee Accts.
- Account Information Changes Via Telephone - Changing PIN's
- Account Information Changes Via Telephone - Credit limit Increase
- Account Information Changes Via Telephone -Disputed Statement
- Account Information Changes Via Telephone - Name
- Account Information Changes Via Telephone -Social Security Number
- Account Number - Fraudulent Use Via Telephone
- Account Takeovers/ Fraudulently Created Accounts
- Accounts - Live and Fraudulent - Detection
- Application - Fraudulent Card Applications - PreScreening
- Application Processing - Access To Account Documentation (paper files)
- Cardholder - Fraudulent Report Of Stolen Card
- Cardholder - Skip Accounts
- Floating - Balance Floating Between Several Accounts And Paid With Credit
- Internal - Collusion Between Card Ctr. Rep & Perpetrator
- Internal - Fee Collections And Funds Disbursements To Other Banks
- Issuing Car - Card Activation
- Merchant - Purchase And Cash Advances On Single Ticket
- Plastic - Additional Card Request
- Plastic Status - Card Intercepted In Mail
- Plastic Status - Counterfeits

- Plastic Status - Lost
- Plastic Status - Reissuing A Card
- Plastic Status - Stolen
- Transaction - ATM Cash Advances
- Transactions - Automatic Billing
- Transactions - Fraudulent Activity/Behavior
- Transaction International
- Transactions - Internet Purchases
- Transactions - Misuse Of Card By Employee
- Transaction - Live Purchases
- Transaction - Payments To Account
- Transaction - Telephone Purchases

**B. Claim 4 has been rejected by the Examiner under 35 USC §102(e) as being unpatentable over Walker, et al. (U.S. patent No. 6,664,987).**

In claim 4, Appellant's set of risks is a function of an individual's profile. In addition to the comments made in above paragraph A, Walker does not disclose a set of risks that are a function of an individual's profile.

**C. Claim 5 has been rejected by the Examiner under 35 USC §102(e) as being unpatentable over Walker, et al. (U.S. patent No. 6,664,987).**

In claim 5, Appellant's set of risks is a function of a business profile. In addition to the comments made in above paragraph A, Walker does not disclose a set of risks that are a function of a business profile.

**D. Claim 6 has been rejected by the Examiner under 35 USC §102(e) as being unpatentable over Walker, et al. (U.S. patent No. 6,664,987).**

In claim 6, Appellant's set of risks is a function of an individual's profile and a business profile. In addition to the comments made in above paragraph A, Walker does not disclose a set of risks that are a function of an individual's profile and a business profile.

**E. Claim 9 has been rejected by the Examiner under 35 USC §102(e) as being unpatentable over Walker, et al. (U.S. patent No. 6,664,987).**

In claim 9, a set of data relative to the credit authorization request is retained in a memory of the data processing system and is utilized to determine the effectiveness of an assessment methodology. In addition to the comments made in above paragraph A, Walker does not disclose utilizing a set of data retained in the memory of a data processing system that is utilized to determine the effectiveness of an assessment methodology.

**F. Claim 10 has been rejected by the Examiner under 35 USC §102(e) as being unpatentable over Walker, et al. (U.S. patent No. 6,664,987).**

In claim 10, the filtering step of claim 1 comprises a credit score filter for eliminating a portion of a population that does not pass through the filter. In addition to the comments made in above paragraph A, Walker does not disclose

a credit score filter that eliminates a portion of a population that does not pass through the filter.

## **IX PRAYER FOR RELIEF**

Appellant respectfully submits that appealed claims 1 –6 and 9 - 10 in this



application are patentable. It is requested that the Board of Appeal overrule the Examiner and direct allowance of the rejected claims.

Respectfully submitted,



Ronald Reichman  
Reg. No. 26,796  
Attorney of Record  
Telephone (203) 924-3854

PITNEY BOWES INC.  
Intellectual Property and  
Technology Law Department  
35 Waterview Drive  
P.O. Box 3000  
Shelton, CT 06484-8000

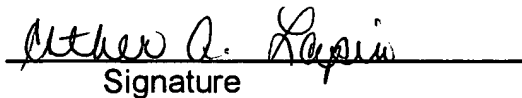
**CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P. O. Box 1450  
Alexandria, VA 22313-1450

On July 29, 2003  
Date of Deposit

Esther A. Lapin  
Name of Rep.

  
Signature

July 29, 2003  
Date

## **APPENDIX OF CLAIMS INVOLVED IN THE APPEAL**

1. A method of managing and assessing a set of risks relative to a financial product, said method being accessed through a data processing system, wherein said data processing system comprises a series of nodes operatively connected with each other, said method comprising the steps of:
  - (a) performing an application processing procedure one or more customers, comprising a check of the creditworthiness of one or more selected customers; and issuing a financial product to one or more of said customers if said selected customer is determined to be creditworthy, thus resulting in an accepted customer, and declining said application if said customer is determined to be not creditworthy;
  - (b) assessing a credit authorization request from a system user, wherein said request is initiated by a use of said financial product;
  - (c) utilizing a predictive modeling routine to perform said assessment;
  - (d) accepting or declining said credit authorization request as based upon an outcome of said assessment;
  - (e) downloading an assessment result to said data processing system for transfer to a database accessible by one or more remote nodes of said system; and
  - (f) applying a fraudi to each assessment and wherein said fraudi is selected from a list of fraudi and wherein each of said fraudi on the list is representative of a defined area of risk.
2. The method of claim 1, wherein said financial product is a credit card.
3. The method of claim 1, wherein said accepted customer is a business entity.

4. The method of claim 1, wherein said accepted customer is an individual and wherein an account is representative of a business affiliation and said set of risks is a function of an individual's profile.
5. The method of claim 1, wherein said accepted customer is an individual and wherein an account is representative of a business affiliation and said set of risks is a function of a business' profile.
6. The method of claim 1, wherein said accepted customer is an individual, and wherein an account is representative of an individual's and a business' affiliation, and said set of risks is a function of an individual's profile and a business' profile.
9. The method of claim 1, wherein a set of data relative to said credit authorization request is retained in a memory of said data processing system and utilized to determine the effectiveness of an assessment methodology.
10. The method of claim 1, wherein a filtering step comprises a credit score filter for eliminating a portion of a population that does not pass through said filter.